UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/564,465	01/12/2006	Yujiro Ito	450100-05166	7460

7590 09/26/2008

William S Frommer
Frommer Lawrence & Haug
745 Fifth Avenue
New York, NY 10151

EXAMINER	
SHOLEMAN, ABU S	
ART UNIT	PAPER NUMBER
4148	
MAIL DATE	DELIVERY MODE
09/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/564,465	ITO ET AL.	
	Examiner	Art Unit	
	ABU SHOLEMAN	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/12/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This instant application having Application No. 10564465 filed on 01/12/2006 is presented for examination by the examiner.

Oath/Declaration

2. The applicants' oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R.1.63.**

Priority

3. As required by **M.P.E.P.201.14(c),** acknowledgement is made of applicant's claim for priority based on applications filed on July 14, 2003 (Japan 2003-273948).

Drawings

4. The drawings were received on 01/12/2006. These drawings are acceptable for examination purposes.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 01/12/2006. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

6. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

7. As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claim 1 recites the limitation "the count" in line 7. There is insufficient antecedent basis for this limitation in the claim.

10. Claim 9 recites the limitation " the held data" in line 15. There is insufficient antecedent basis for this limitation in the claim.

11. Claim 10 recites the limitation "the held data" in line 10. There is insufficient antecedent basis for this limitation in the claim.

12. Claim 11 recites the limitation "the held data" in line 11. There is insufficient antecedent basis for this limitation in the claim.

13. Claim 12 recites the limitation "the held data" in line 27 and 20. There are insufficient antecedent basis for this limitation in the claim.

14. Claim 20 recites the limitation "the held data" in line 6 and line 23. There are insufficient antecedent basis for this limitation in the claim.

15. Claim 21 recites the limitation "the held data" in line 18 and line 7. There are insufficient antecedent basis for this limitation in the claim.

16. Claim 22 recites the limitation "the held data" in line 3 and line 19. There are insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

17. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

SOFTWARE PER SE

18. **Claim 10** is rejected under 35 U.S.C. 101 as directed to non-statutory subject matter of software, *per se*. The claim lacks the necessary physical articles or objects to constitute a machine or manufacture within the meaning of 35 U.S.C. 101. It is clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. It is at best, function descriptive material *per se*.

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." Both types of "descriptive material" are non-statutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994).

Merely claiming non-functional descriptive material, i.e., abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See *Diehr*, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in *Benson* were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.").

In this case, applicant has claimed a "an encryption program" of the kind set forth characterized in that an encryption program caused a computer device for execution that is implemented by a software language; this implied that the encryption program was never actually executed yet, thus, applicant is claiming a system of software, per se, lacking the hardware necessary to realize any of the underlying functionality. Therefore, claim 10 is directed to non-statutory subject matter as an encryption program, per se, i.e. the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as

they are not “acts” being performed. Such claimed an encryption programs do not define any structural and functional interrelationships between an encryption program and other claimed elements of a computer device , which permit an encryption program's functionality to be realized.

19. **Claim 11** is rejected under 35 U.S.C. 101 as directed to non-statutory subject matter of software, *per se*. The claim lacks the necessary physical articles or objects to constitute a machine or manufacture within the meaning of 35 U.S.C. 101. It is clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. It is at best, function descriptive material *per se*.

Descriptive material can be characterized as either “functional descriptive material” or “nonfunctional descriptive material.” Both types of “descriptive material” are non-statutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994).

Merely claiming non-functional descriptive material, i.e. abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See *Diehr*, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in *Benson* were unpatentable as abstract ideas because

"[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.").

In this case, applicant has claimed a "a record medium" of the kind set forth characterized in that an encryption program that is implemented by a software language and this encryption program causing execution; this implied that the encryption program was never actually executed yet, thus, applicant is claiming a system of software, per se, lacking the hardware necessary to realize any of the underlying functionality. Therefore, claim 11 is directed to non-statutory subject matter as computer program, per se, i.e. the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed a record medium programs do not define any structural and functional interrelationships between a record medium and other claimed elements of a computer readable medium, which permit a record medium's functionality to be realized.

20. **Claim 21** is rejected under 35 U.S.C. 101 as directed to non-statutory subject matter of software, *per se*. The claim lacks the necessary physical articles or objects to constitute a machine or manufacture within the meaning of 35 U.S.C. 101. It is clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. It is at best, function descriptive material *per se*.

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." Both types of "descriptive material" are

non-statutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994).

Merely claiming non-functional descriptive material, i.e., abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See *Diehr*, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in *Benson* were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.").

In this case, applicant has claimed a "an decryption program" of the kind set forth characterized in that an decryption program caused a computer device for execution that is implemented by a software language; this implied that the decryption program was never actually executed yet, thus, applicant is claiming a system of software, per se, lacking the hardware necessary to realize any of the underlying functionality. Therefore, claim 21 is directed to non-statutory subject matter as an decryption program, per se, i.e. the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed an decryption programs do not define any structural and functional interrelationships between an decryption program and other

claimed elements of a computer device, which permit an decryption program's functionality to be realized.

21. **Claim 22** is rejected under 35 U.S.C. 101 as directed to non-statutory subject matter of software, *per se*. The claim lacks the necessary physical articles or objects to constitute a machine or manufacture within the meaning of 35 U.S.C. 101. It is clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. It is at best, function descriptive material *per se*.

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." Both types of "descriptive material" are non-statutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994).

Merely claiming non-functional descriptive material, i.e. abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See *Diehr*, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in *Benson* were unpatentable as abstract ideas because

"[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.").

In this case, applicant has claimed a "a record medium" of the kind set forth characterized in that an decryption program that is implemented by a software language and this decryption program causing execution; this implied that the decryption program was never actually executed yet, thus, applicant is claiming a system of software, per se, lacking the hardware necessary to realize any of the underlying functionality. Therefore, claim 22 is directed to non-statutory subject matter as computer program, per se, i.e. the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed a record medium programs do not define any structural and functional interrelationships between a record medium and other claimed elements of a computer readable medium, which permit a record medium's functionality to be realized.

Claim Rejections - 35 USC § 102

22. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

23. Claims 1, 2, 3, 9, 10, 11, 12, 13, 14, 20, 21 and 22 are rejected under 35 U.S.C 102(b) as being anticipated by et al (Patent No:5345508)(hereinafter Lynn).

As per claim 1, Lynn discloses "An encryption apparatus, comprising: hold means for holding a part or all input data with a trigger signal and resetting the held data with a reset signal" as (column 5, line 36-39, A logical gate combine the plaintext data with a PN sequence and line 1-2, reset signal generated new sequence of data); "one or a plurality of counters that count up or count down the count values with a the trigger signal and reset the count values to predetermined values with the reset signal" as (column 6,line 5-7, counter is decrementing with each sequence processed and line 2, counter contents reaches zero); "encryption means for encrypting the data held by the hold means and one or a plurality of count values of the one or plurality of counters" as(column 1 line 59-62, The PN sequence is then combined with the plaintext message to be encrypted to produce a sequence of cipher text); " calculation means for calculating the output of the encryption means and input data that are input from the outside according to a predetermined rule, encrypting the input data and outputting the encrypted data" as (column 5, line 56-60, counter is operated by count signal into counter as each new data sequence and line 67-69, the decrement the counter contents by the encrypting proceeds); "a path that inputs a part or all the encrypted data that are output from the calculation means to the hold means" as (column 5, line 12-15 the cipher text output information is transmitted to receiver through a channel); " signal generation means for generating the trigger signal and the rest signal supplied to the

hold means and the one or plurality of counters according to a predetermined rule and or at predetermined timing" as (column 4 line 54-60, vector is produced by IV(signal) generator and utilized by transmitter that hold data and column 6, line 3-4, counter is resetting the IV(signal) generator).

24. **As per claim 2**, Lynn discloses " wherein a fixed value is input to the encryption means" as (column 4, line 47-48, encryption key would be unique), and "wherein the encryption means encrypts the fixed value, the data held by the hold means, and the one or plurality of count values" as (column 5, line 38-39, counter generator IV and key are producing PN sequence that is cached with plaintext data to produce cipher text).

25. **As per claim 3,** Lynn discloses "Wherein the reset signal that resets the data held by the hold means is supplied to the hold means at timing in synchronization with the reset signal supplied to at least one of the one or plurality of counters" as (column 5, line 1-5, reset signal that a new sequence of data to be generated and counter count).

26. **As per claim 9**, Lynn discloses 'An encryption method, comprising the steps of : holding a part or all input data with a trigger signal and resetting the held data with a reset signal " as (column 5, line 36-39, A logical gate combine the plaintext data with PN sequence and line 1-2, reset signal generated new sequence of data); " counting up or down the values with the trigger signal and resetting the count values to predetermined values with the reset signal" as (count, line 5-7, counter is decrementing with each sequence processed and line 2, counter contents reaches zero); "encrypting the data held by the hold step and one or a plurality of count values at the count step" as (column 1, line 59-62, The PN sequence is then combined with the plaintext message

to be encrypted to produce a sequence of cipher text); "calculating the output of the encryption step and input data that are input from the outside according to a predetermined rule, encrypting the input data, and outputting the encrypted data' as (column 5, line 56-60, counter is operated by count signal into counter as each new data sequence and line 67-69, the decrement the counter contents by the encrypting proceeds); "inputting a part or all the encrypted data that are output at the calculation step to the hold step" as (column 5, line 12-15, the cipher text output information is transmitted to receiver through a channel); "generating the trigger signal and the reset signal supplied to the hold step and the count step according to a predetermined rule and / or at predetermined timing" as (column 4, line 54-60, vector is produced by IV(signal) generator and utilized by transmitter that hold data and column 6, line 3-4, counter is resetting the IV(signal) generator).

27. **As per claim 10,** Lynn discloses " An encryption program that causes a computer device to execute a encrypted method" as (column 7, line 29-31, the encryption system is consist of programmed instructions implemented on computer), 'the encryption method comprising the steps of" holding a part or all input data with a trigger signal and resetting the held data with a reset signal' as (column 5, line 36, A logical gate combine the plaintext data with PN sequence and line 1-2 , reset signal generated new sequence of data); " counting up or down the count values with the trigger signal and resetting the count values to predetermined values with the reset signal " as (Column 6, line 5-7, Counter is decrementing with each sequence processed and line 2, counter contents reaches zero); "encrypting the data held at the

hold step and one or a plurality of count values at the count step" as (column 1, line 59-62, The PN sequence is then combined with plaintext message to be encrypted to produce a sequence of cipher text); "calculating the output at the encryption step and input data that are input from the outside according to a predetermined rule, encrypting the input data and outputting the encrypted data" as (column 5, line 56-60, counter is operated by count signal into counter as each new data sequence and the line 67-69, the decrement the counter contents by the encrypting proceeds); "inputting a part or all the encrypted data that are output at the calculation step to the hold step" as (column5, line 12-15, the cipher text output information is transmitted to receiver through a channel); "generating the trigger signal and the reset signal supplied to the hold step and the count step according to a predetermined rule and/or at predetermined timing" as (column 4, line 54-60, vector is produced by IV(signal) generator and utilized by transmitter that hold data and column 6, line 3-4, counter is resetting the IV(signal) generator).

28. **As per claim 11**, Lynn discloses " A record medium from which a computer device can read an encryption program that causes the computer device to execute an encrypted method" as (column 7, line 52-53, computer execute program instruction from program memory), "the encryption method comprising the steps of : holding a part or all input data with a trigger signal and resetting the held data with a reset signal " as (column 5, line 36-39, a logical gate combine the plain text data with a PN sequence and line 1-2, reset signal generated new sequence of data); "counting up or down the count values with the trigger signal and resetting the count values to predetermined values

with the reset signal" as (column 6, line 5-7, counter is decrementing with each sequence processed and line 2, counter contents reaches zero); " encrypting the data held by the hold step and or a plurality of count values at the count step" as (column 1, line 50-62, The PN sequence is then combined with the plaintext message to be encrypted to produce a sequence of cipher text);"calculating the output at the encryption step and input data that are input from the outside according to a predetermined rule, encrypting the input data , and outputting the encrypted data" as (column 5, line 56-60, counter is operated by count signal into counter as each new data sequence and line 76-69, the decrement the counter contents by the encrypting proceeds); " Inputting a part of all the encrypted data that are output at the calculation step to the hold step" as (column 5, line 12-15, the cipher text output information is transmitted to receiver through a channel); " generating the trigger signal and the reset signal supplied to the hold step and the count step according to the predetermined rule and or at predetermined timing" as (column 4, line 54-60, vector is produced by IV(signal) generator and utilized by transmitter that hold data and column 6, line 3-4, counter is resetting the IV(signal) generator).

29. **As per claim 12,** Lynn discloses ' A decryption apparatus that decrypts encrypted data encrypted by an encryption apparatus that comprises hold means for holding a part or all input data with a trigger signal and resetting the held data with a reset signal" as (column 5, line 36-39, A logical gate combine the plain text data with PN sequence and line 1-2, reset signal generated new sequence of data); " one or a plurality of counters that count up or count down the count values with the trigger signal

and rest the count values to predetermined values with the reset signal' as (column 6, line 5-7, counter is decrementing with each sequence processed and line 2, counter contents reaches zero); " encryption mean for encrypting the data held by the hold mean and one or a plurality of count values of the one or plurality of counters" as (column 1, line 59-62, The PN Sequence is then combined with the plaintext message to be encrypted to produce a sequence of cipher text);" calculating means for calculating the output of the encryption means and input data that are input from the outside according to a predetermined rule, encrypting the input data , and outputting the encrypted data' as (column 5, line 56-60, counter is operated by count signal into counter as each new data sequence, and line 67-69, then decrement the counter contents by the encrypting processed); "a path that inputs a part or all the encrypted data that are output from the calculation means to the hold means" as (column 5, line 12-15 the cipher text output information is transmitted to receiver through a channel); " signal generation means for generating the trigger signal and the reset signal supplied to the hold means and the one or plurality of counters according to a predetermined rule and or at the predetermined timing" as (Column 4, line 54-60, vector is produced by IV(signal) generator and utilized by transmitter that hold data and column 6, line 3-4, counter is resetting the IV(signal) generator);"the decryption apparatus comprising" hold means or holding a part or all input data with a trigger signal and resetting the held data with a reset signal' as (column 7, line 15-17,data is held on logical gate 64 with selected sequence signal); " one or a plurality of counters that count up or count down the count values with the trigger signal and reset the count values to predetermined

values with the reset signal " as (column 6, line 5-7, transmitter and receiver are self synchronized, counter is decrementing with each sequence processed and line 2, counter contents reaches zero); " encryption means for encrypting the data held by the hold means and one or a plurality of count values of the one or plurality of counters" as (column 1, line 59-62, The PN sequence is then combined with the plaintext message to be encrypted to produce a sequence of cipher text); " calculation means for calculating the out put of the encryption means and input data that are input from the outside according to a predetermined rule , encrypting the input data, and outputting the encrypted data" as (column 5, line 56-60, counter is operated by count signal into counter as each new data sequence and line 76-69, the decrement the counter contents by the encrypting proceeds); " a path that inputs a part or all the encrypted data that are output from the calculation means to the hold means" as (column 5, line 12-15, the cipher text output information is transmitted to receiver through a channel); " signal generation means for generating the trigger signal and the reset signal supplied to the h old means and the one or plurality of counters according to a predetermined rule and /or at predetermined timing" as (column 4, line 54-60, Vector is produced by IV(signal) generator and utilized by transmitter that hold data and column 6, line 3-4, counter is resetting the IV(signal) generator).

30. **As per claim 13**, Lynn discloses "Wherein a fixed value is input to the encryption means" as (column 4, line 47-48, encryption key would be unique), and "wherein the encryption means encrypts the fixed value, the data held by the hold means, and the

one or plurality of count values' as (column 5, line 38-39, counter generator IV and key are producing PN sequence that is cached with plain text data to produce cipher text).

31. **As per claim 14,** Lynn discloses " Wherein the reset signal that resets the data held by the hold means is supplied to the hold means at timing in synchronization with the reset signal supplied to at least one of the one or plurality of counters" as (column 5, line 1-5, reset signal that a new sequence of data to be generated and counter count).

32. **As per claim 20,** Lynn discloses " A decryption method of decrypting encrypted data encrypted in an encryption method" as (column 6, line 24-27, a cipher text is decoded to produced a plaintext), " the encryption method comprise the step of holding a part or all input data with a trigger signal and resetting the held data with a reset signal" as (column 5, line 36-39, a logical gate combine the plaintext data with PN Sequence and line 1-2, reset signal generated new sequence of data); " counting up or down the count values with the trigger signal and resetting the count values to predetermined values with reset signal" as (column 6, line 5-7, counter is decrementing with each sequence processed and line 2, counter contents reaches zero); " encrypting the data held at the hold step and one or a plurality of cont values at the count step" as (column 1, line 59-62, The PN sequence is then combined with the plaintext message to be encrypted to produce a sequence of cipher text); " calculating the output at the encryption step and input data that are input from the outside according to a predetermined rule , encrypting the input data , and outputting the encrypted data" as (column 5, line 56-60, counter is operated by count signal into counter as each new data sequence and line 67-69, the decrement the counter contents by the encrypting

proceeds); " inputting a part or all the encrypted data that are output at the calculation step to the hold step" as (column 5, line 12-15, the cipher text output information is transmitted to receiver through a channel); " generating the trigger signal and the reset signal supplied to the hold step and the count step according to a predetermined rule and or at predetermined timing" as (column 4, line 54-60, vector is produced by IV(signal) generator and utilized by transmitter that hold data and column 6, line 3-4 , counter is resetting the IV(signal) generator)," The decryption apparatus comprising: hold means for holding a part or all input data with a trigger signal and resetting the held data with a reset signal" as (column 7, line 15-17, data is held in logical gate with the selected sequence signal); "counting up or down the count values with the trigger signal and resetting the count values to predetermined values with the reset signal" as (column 6, line 5-7, transmitter and receiver are self synchronized , counter is decrementing with each sequence processed and line 2, counter contents reaches zero); " encrypting the data held at the hold step or one or plurality of count values at the count step(column 1, line 59-62, The PN sequence is then combined with the plaintext message to be encrypted to produce a sequence of cipher text);" calculating the output of the encryption step and input data that are input from the outside according to the predetermined rule, encrypting the input data and outputting the encrypted data" as (column 5, line 56-69, the decrement the counter contents by the encrypting proceeds);" inputting a part or all the encrypted data that are input from outside to the hold mean" as (column 5, line 12-15, the cipher text output information is transmitted to receiver through a channel); " generating the trigger signal and the reset

signal supplied to the hold step to the count step according to a predetermined rule and or at predetermined timing " as (column 4, line 54-60, Vector id produced by IV(signal) generator and utilized by transmitter that hold data and column 6, line 3-4, counter is resetting the IV(signal) generator).

33. **As per claim 21**, Lynn discloses" An decryption program that causes a computer device to execute an encrypted method of decrypting encrypted data encrypted in an encrypted method" as (column 7, line 29-31, the decryption system is consist of programmed instructions implemented on computer), 'the encryption method comprising the steps of" holding a part or all input data with a trigger signal and resetting the held data with a reset signal' as (column 5, line 36-39, A logical gate combine the plaintext data with PN sequence and line 1-2 , reset signal generated new sequence of data); " counting up or down the count values with the trigger signal and resetting the count values to predetermined values with the reset signal " as (Column 6, line 5-7, Counter is decrementing with each sequence processed and line 2, counter contents reaches zero); "encrypting the data held at the hold step and one or a plurality of count values at the count step" as (column 1, line 59-62, The PN sequence is then combined with plaintext message to be encrypted to produce a sequence of cipher text); "calculating the output at the encryption step and input data that are input from the outside according to a predetermined rule, encrypting the input data and outputting the encrypted data" as (column 5, line 56-60, counter is operated by count signal into counter as each new data sequence and the line 67-69, the decrement the counter contents by the encrypting proceeds); "inputting a part or all the encrypted data that are

output at the calculation step to the hold step" as (column5, line 12-15, the cipher text output information is transmitted to receiver through a channel); "generating the trigger signal and the reset signal supplied to the hold step and the count step according to a predetermined rule and/or at predetermined timing" as (column 4, line 54-60, vector is produced by IV(signal) generator and utilized by transmitter that hold data and column 6, line 3-4, counter is resetting the IV(signal) generator),the decryption method comprising the steps of holding a part or all input data with a trigger signal and resetting the held data with a reset signal" as (column 5, line 36-39, A logical gate combine the plaintext data with PN sequence and line 1-2 , reset signal generated new sequence of data); "counting up or down the count values with trigger signal and resetting the count values to predetermined values with the reset signal" as (column 6 , line 5-7, counter is decrementing with each sequence processed and line , counter contents reaches zero); "encrypting the data held at the hold step and one or a plurality of count values at the count step" as (column 1, line 59-62, the PN Sequence is then combined with the plaintext message to be encrypted to produce a sequence of cipher text); " calculating the output at the encryption step and input data that are input from the outside according to a predetermined rule , encrypting the input data and outputting the encrypted data' as (column 5, line 56-60, counter is operated by count signal into counter as each new data sequence and line 67-69, the decrement the counter contents by the encrypting proceeds); "Inputting a part or all the encrypted data that are output at the calculation step or the hold step" as (column 5, line 12-15, the cipher text output information is transmitted to receiver through a channel); " generating the trigger signal

supplied to the hold step and the count step according to a predetermined rule and or at predetermined timing" as (column 4, line 54-60, vector is produced by IV(signal) generator and utilized by transmitter that hold data and column 6, line 3-4, counter is resetting the IV(signal) generator).

34. **As per claim 22**, Lynn discloses " A record medium from which a computer device can read an encryption program that causes the computer device to execute an encrypted method" as (column 7, line 52-53, computer execute program instruction from program memory), "the encryption method comprising the steps of : holding a part or all input data with a trigger signal and resetting the held data with a reset signal " as (column 5, line 36, a logical gate combine the plain text data with a PN sequence and line 1-2, reset signal generated new sequence of data); "counting up or down the count values with the trigger signal and resetting the count values to predetermined values with the reset signal" as (column 6, line 5-7, counter is decrementing with each sequence processed and line 2, counter contents reaches zero); " encrypting the data held by the hold step and or a plurality of count values at the count step" as (column 1, line 50-62, The PN sequence is then combined with the plaintext message to be encrypted to produce a sequence of cipher text);"calculating the output at the encryption step and input data that are input from the outside according to a predetermined rule, encrypting the input data , and outputting the encrypted data" as (column 5, line 56-60, counter is operated by count signal into counter as each new data sequence and line 76-69, the decrement the counter contents by the encrypting proceeds); " Inputting a part of all the encrypted data that are output at the calculation

step to the hold step" as (column 5, line 12-15, the cipher text output information is transmitted to receiver through a channel); " generating the trigger signal and the reset signal supplied to the hold step and the count step according to the predetermined rule and or at predetermined timing" as (column 4, line 54-60, vector is produced by IV(signal) generator and utilized by transmitter that hold data and column 6, line 3-4, counter is resetting the IV(signal) generator), the decryption method comprising the steps of holding a part or all input data with a trigger signal and resetting the held data with a reset signal" as (column 5, line 36-39, A logical gate combine the plaintext data with PN sequence and line 1-2 , reset signal generated new sequence of data); "counting up or down the count values with trigger signal and resetting the count values to predetermined values with the reset signal" as (column 6 , line 5-7, counter is decrementing with each sequence processed and line , counter contents reaches zero); "encrypting the data held at the hold step and one or a plurality of count values at the count step" as (column 1, line 59-62, the PN Sequence is then combined with the plaintext message to be encrypted to produce a sequence of cipher text); " calculating the output at the encryption step and input data that are input from the outside according to a predetermined rule , encrypting the input data and outputting the encrypted data' as (column 5, line 56-60, counter is operated by count signal into counter as each new data sequence and line 67-69, the decrement the counter contents by the encrypting proceeds); "Inputting a part or all the encrypted data that are output at the calculation step or the hold step" as (column 5, line 12-15, the cipher text output information is transmitted to receiver through a channel); " generating the trigger signal

supplied to the hold step and the count step according to a predetermined rule and or at predetermined timing" as (column 4, line 54-60, vector is produced by IV(signal) generator and utilized by transmitter that hold data and column 6, line 3-4, counter is resetting the IV(signal) generator).

Claim Rejections - 35 USC § 103

35. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

36. **Claims 4 and 5** are rejected under 35 U.S.C.103(a) as being unpatentable over Lynn et al (Patent No: US 5345508) (hereinafter Lynn) in view of Tehranchi (Patent No: 7242772 B1) (hereinafter Tehranchi).

37. **As per claim 4**, Lynn discloses "The encryption apparatus as set forth in claim 1" as(see rejection of above claim 1), but does not disclose "wherein the input data are picture data , and wherein the reset signal that resets the hold means is in synchronization with the picture data".

However, Tehranchi discloses "wherein the input data are picture data" as (column 1 , line 58, motion picture data for encrypted , and " wherein the reset signal that resets the hold means is in synchronization with the picture data" as (column 3, line 16-

19, synchronize key to the data, where key is generated by reset signal for each new sequence of picture data).

Lynn and Tehranchi are analogous arts because they are the same field of endeavor of apparatus of encryption of data stream.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Lynn by including a picture data instead of plaintext that taught by Tehranchi in order to prevent the data piracy of digital motion pictures (column 1, line 25-28).

38. **As per claim 5,** Tehranchi discloses “wherein the reset signal that resets the hold means is in synchronization with each line of the picture data" as (column 5, line 26-29, an encryption key that is produced by reset signal synchronized with a each single block of data).

39. **As per claim 6,** Lynn discloses “The encryption apparatus as set forth in claim 1" as (see rejection of above claim 1), but fails to disclose “wherein the input data are picture data, and wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with the picture data".

However, Tehranchi discloses “wherein the input data are picture data" as (column 1, line 58-60, motion picture data for encrypted) and "wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with the

picture data" as (Column 7, line 5-6, a plurality of keys is used to encrypt a plurality of blocks).

Lynn and Tehranchi are analogous arts because they are the same field of endeavor of apparatus of encryption of data stream.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Lynn by including a picture data instead of plaintext and adding a counter for reset signal that taught by Tehranchi in order to prevent the data piracy of digital motion pictures (column 1, line 25-28).

40. **Claims 7 and 8** are rejected under 35 U.S.C.103(a) as being unpatentable over Lynn et al (Patent No: US 5345508) (hereinafter Lynn) in view of Tehranchi (Patent No: 7242772 B1) (hereinafter Tehranchi) and further in view of in view of Hosford et al (Patent No: 5966450) (hereinafter Hosford).

41. **As per claim 7**, Lynn discloses " The encryption apparatus as set forth in claim 6" as (see rejection of above claim 6), but Lynn and Tehranchi do not disclose "wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with each frame of the picture data" .

However, Hosford discloses "wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with each frame of the picture data"

as (column 3, line 51-55, resetting the frame counter comprises setting the frame counter to the stored initial value and frame counter is synchronization with each other).

Lynn, Tehranchi and Hosford are analogous arts because they are the same field of endeavor of apparatus of encryption of data stream.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Lynn in view of Tehranchi by including a counter for each from frame of picture data instead of plaintext that taught by Hosford it would provide an independently each frame in transmission station to receiving station as a result it would be difficult to obtain for an eavesdropper (column 3, line 56-60).

42. **As per claim 8,** Lynn discloses " The encryption apparatus as set forth in claim 6" as (see rejection of above claim 6), but Lynn and Tehranchi do not disclose " wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with each line of the picture data ".

However, Hosford discloses " wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with each line of the picture data" as (column 3, line 3-5, frame on a bit-by bit basis to produce en encrypted frame).

Lynn, Tehranchi and Hosford are analogous arts because they are the same field of endeavor of apparatus of encryption of data stream.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Lynn in view of Tehranchi by

including a counter for each from line of picture data instead of plaintext that taught by Hosford it would provide an independently each line in transmission station to receiving station as a result it would be difficult to obtain for an eavesdropper (column 3, line 56-60).

43. **Claims 15 and 16** are rejected under 35 U.S.C.103(a) as being unpatentable over Lynn et al (Patent No: US 5345508) (hereinafter Lynn) in view of Tehranchi (Patent No: 7242772 B1) (hereinafter Tehranchi).

44. **As per claim 15**, Lynn discloses "The decryption apparatus as set forth in claim 1" as(see rejection of above claim 12), But does not disclose "wherein the encrypted data are encrypted picture data , and wherein the reset signal that resets the hold means is in synchronization with the picture data".

However, Tehranchi discloses "wherein the encrypted data are encrypted picture data" as (column 1 , line 58-60, motion picture data for encrypted , and " wherein the reset signal that resets the hold means is in synchronization with the picture data" as (column 3, line 16-19, synchronize key to the data, where key is generated by reset signal for each new sequence of picture data).

Lynn and Tehranchi are analogous arts because they are the same field of endeavor of apparatus of decryption of data stream.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Lynn by including a picture data instead of plaintext that taught by Tehranchi in order to prevent the data piracy of digital motion pictures (column 1, line 25-28).

45. **As per claim 16**, Tehranchi discloses “wherein the reset signal that resets the hold means is in synchronization with each line of the picture data" as (column 5, line 26-29, an encryption key that is produced by reset signal synchronized with a each single block of data).

46. **As per claim 17**, Lynn discloses "The decryption apparatus as set forth in claim 1” as(see rejection of above claim 12), but fails to disclose “wherein the encrypted data are encrypted picture data , and wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with the picture data".

However,Tehranchi discloses “wherein the encrypted data are encrypted picture data" as (column 1, line 58, motion picture data for encrypted) and "wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with the picture data" as (Column 7, line 5-6, a plurality of keys is used to encrypt a plurality of blocks).

Lynn and Tehranchi are analogous arts because they are the same field of endeavor of apparatus of decryption of data stream.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Lynn by including a picture data instead of plaintext with a counter of each line of the picture that taught by Tehranchi it would enforce more protection of each individual line of the the data piracy of digital motion pictures (column 1, line 25-28).

47. **Claims 18 and 19** are rejected under 35 U.S.C.103(a) as being unpatentable over Lynn et al (Patent No: US 5345508) (hereinafter Lynn) in view of Tehranchi (Patent No: 7242772 B1) (hereinafter Tehranchi) and further in view of in view of Hosford et al (Patent No: 5966450) (hereinafter Hosford).

48. **As per claim 18**, Lynn discloses " The decryption apparatus as set forth in claim 17" as (see rejection of above claim 17), but Lynn and Tehranchi do not disclose "wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with each frame of the picture data" .

However, Hosford discloses "wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with each frame of the picture data" as (column 3, line 51-55, resetting the frame counter comprises setting the frame counter to the stored initial value and frame counter is synchronization with each other).

Lynn, Tehranchi and Hosford are analogous arts because they are the same field of endeavor of apparatus of decryption of data stream.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Lynn in view of Tehranchi by including a counter for each from frame of picture data instead of plaintext that taught by Hosford it would provide an independently each frame in transmission station to receiving station as a result it would be difficult to obtain for an eavesdropper (column 3, line 56-60).

49. **As per claim 19**, Lynn discloses " The decryption apparatus as set forth in claim 17" as (see rejection of above claim 17), but fails to disclose " wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with each line of the picture data".

However, Hosford discloses " wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with each line of the picture data" as (column 3, line 3-5, frame on a bit-by bit basis to produce en encrypted frame).

Lynn, Tehranchi and Hosford are analogous arts because they are the same field of endeavor of apparatus of decryption of data stream.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Lynn in view of Tehranchi by including a counter for each line of picture data instead of plaintext that taught by Hosford it would provide an independently each line in transmission station to receiving station as a result it would be difficult to obtain for an eavesdropper (column 3, line 56-60).

Conclusion

50. The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See MPEP 707.05(c).

51. The following reference teaches execution of trial data.

US 5444781

US 5488659

US 6314188

US 4642688

US 5058157

US 5588075

Concrete security Analysis of CTR_OFB and CTR-CFB Modes of Operation

52. Any inquiry concerning this communication or earlier communication form the examiner should be directed to Abu Sholeman whose telephone number is (571)270-7314. the examiner can normally be reached on Monday to Friday 8:30 AM to 5.00PM.

If attempts to reach the above noted Examiner by telephone are un successful, the Examiner's supervisor, Thomas Pham, can be reached at the following telephone number (571)2272-3689.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status

information for published applications may be obtained from the either Private PAIR or public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pari-direct.uspto.gov. Should your have questions on access to the Private PAIR system, contact the Electronic Business Center(EBC) at 866-217-9197(toll-free).

September 18, 2008

Abu Sholeman
Examiner
Art Unit 4148

/THOMAS PHAM/

Supervisory Patent Examiner, Art Unit 4148